(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 577 704**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **85 02402**

(51) Int Cl⁴ : G 06 K 9/62; G 06 F 7/48; G 07 D 7/00.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 18 février 1985.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 34 du 22 août 1986.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *SYSTEMES SUD, Société anonyme, AUTHIE Jean-Paul et CASSADO Manuel.* — FR.

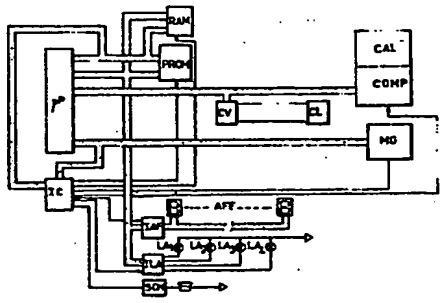
(72) Inventeur(s) : Gilbert Delpech, Jean-Paul Authie et Manuel Cassado.

(73) Titulaire(s) :

(74) Mandataire(s) : Cabinet Barre, Gatti, Laforgue.

(54) Procédé et machine pour la vérification de chèques bancaires ou postaux.

(57) L'invention concerne un procédé et une machine de vérification de la légalité d'émission d'un chèque bancaire ou postal en vue de permettre au bénéficiaire de détecter un chèque volé. La machine comprend un microprocesseur (μP), des moyens de saisie du numéro de compte inscrit sur le chèque (MG), des moyens de conversion en binaire (μP), des moyens de calcul logique (CAL) adaptés pour faire correspondre à l'ensemble antécédent des numéros de comptes de titulaires en base binaire, l'ensemble image des nombres binaires à au plus 14 bits, un système d'entrée décimal (CL) pour l'introduction d'un code confidentiel décimal à 4 chiffres, des moyens de conversion du code en base binaire (CV), des moyens de mémorisation temporaire dudit code (RAM), des moyens logiques (COMP) de comparaison du résultat issu des moyens de calcul et du code en base binaire mémorisé, et des moyens avertisseurs AFF; SON; LA_3; LA_4 pour traduire sous forme simple les résultats de la comparaison.



FR 2 577 704 - A1

Vente des fascicules à l'IMPRIMERIE NATIONALE, 27, rue de la Convention — 75732 PARIS CEDEX 15

PROCEDE ET MACHINE POUR LA VERIFICATION DE CHEQUES BANCAIRES OU POSTAUX

L'invention concerne un procédé de vérification de la légalité d'émissions de chèques bancaires ou postaux en vue de permettre aux bénéficiaires de détecter les chèques volés ; elle s'applique pour la vérification de chèques de type traditionnel. L'invention s'étend également, d'une part, à une machine électronique de vérification de chèques, mise à la disposition des bénéficiaires (la plupart du temps des commerçants), d'autre part, à une machine électronique mise à la disposition des organismes bancaires en vue de permettre la mise en oeuvre du procédé.

On sait que la fraude au détriment des commerçants, qui consiste à payer une marchandise au moyen d'un chèque volé, porte sur des sommes considérables de plus en plus importantes et a pour conséquence une véritable remise en cause de la fiabilité du chèque dans le secteur du petit commerce ; le trafic des carnets de chèques volés allant de pair avec celui des cartes d'identité, l'obligation faite au signataire du chèque de prouver son identité ne réduit pas la fraude dans une proportion très notable. Un remède récent a été mis en place consistant pour le commerçant à consulter une banque de données des chèques volés ; toutefois l'importance de la fraude interdit en pratique l'établissement d'une banque de données exhaustive nationale et, même sur le plan régional, ces banques de données sont très lourdes à gérer et à actualiser.

Par ailleurs, un problème similaire existant pour les cartes de billetterie a été résolu grâce à un système d'attribution d'un code confidentiel au titulaire de la carte, code possédant généralement 4 chiffres décimaux de façon à être facilement mémorisable par le titulaire, avec une très faible probabilité d'être retrouvé au hasard. Ce système consiste à ajouter une information numérique sur la carte, dite "information inscrite", ayant le même nombre de chiffres que le code confidentiel, et à faire correspondre à cette information inscrite un code confidentiel différent de cette information, que seul le titulaire connaît ; lors de l'utilisation de la carte, le titulaire doit entrer son code confiden-

tiel et une vérification de concordance permet de valider ou non l'opération de retrait d'argent dans l'appareil de distribution automatique.

On pourra notamment se reporter aux brevets US n° 4.048.475 ou brevet GB n° 2.020.074, qui portent sur des systèmes de ce type et fournissent des procédés spécifiques pour faire correspondre de façon bi-univoque l'ensemble des codes confidentiels à 4 chiffres et l'ensemble des informations inscrites à 4 chiffres.

Toutefois, pour être efficace, un tel système ne doit pas permettre à un fraudeur de retrouver notamment par une simulation informatique, le code confidentiel à partir de l'information inscrite. Dans ces conditions, la fonction de correspondance doit être inviolable : dans le cas des cartes de crédit, cette garantie est fournie, soit en ajoutant une ou plusieurs informations paramétrées se rapportant au passé de la carte (notamment nombre d'utilisations de la carte modifiant les paramètres de la fonction), soit en établissant une table de correspondance aléatoire de toutes les informations inscrites et de tous les codes confidentiels attachés à celles-ci.

Mais, ces systèmes ne sont pas applicables à la vérification des chèques et le problème de la fraude n'est pas résolu dans ce cas malgré l'importance des sommes en jeu et le caractère relativement ancien des systèmes conçus pour les cartes. En effet, un chèque n'est utilisé qu'une fois et aucun paramètre ne peut donc être déduit de son passé. De plus, la mémorisation d'une table aléatoire complète de correspondance entre tous les codes confidentiels et toutes les informations inscrites fait nécessairement appel à une technologie avancée ("circuit dit à la demande, de type "L.S.I.") et exige des moyens dont le coût est incompatible avec l'investissement envisageable par la plupart des commerçants.

En outre, le caractère inviolable d'une telle table aléatoire est optimum vis-à-vis d'une simulation informatique, puisqu'il n'y a pas de fonction logique entre code confidentiel et information inscrite et que seule la connaissance complète de la table permet de faire la relation. Toutefois, ce système est peu fiable s'il est possible d'accéder facilement à

la table : dans ces conditions, si un tel système est admissible dans un organisme bancaire (car les moyens informatiques qui supportent la table ne sont pas accessibles au public), il ne l'est plus par contre dans le cas d'une diffusion auprès des commerçants, l'accès à la table devenant facile pour quiconque, par une lecture informatique qui n'exige que des moyens relativement élémentaires.

Par ailleurs, une demande de brevet française n° 81.00839 évoque un système de contrôle de cartes de billetterie, du type ci-dessus indiqué et suggère son application à la vérification "de l'identité d'un client réglant son achat par chèque" (p. 6, ligne 1). Toutefois, ce brevet reste au niveau d'une simple allusion et ne fournit aucun moyen pour résoudre effectivement le problème dans le cas des chèques.

Il convient de souligner que l'application aux chèques d'un système de vérification de ce type soulève une autre difficulté venant s'ajouter à celles déjà évoquées (inviolabilité d'accès de la loi de correspondance, aussi bien physique que logique, coût compatible avec une mise du système à la disposition de chaque commerçant). En effet, le système des chèques bancaires est trop lourd et trop figé pour pouvoir être aisément modifié et il est difficilement concevable de l'aménager pour ajouter sur tous les chèques une ou des informations permettant de contrôler le code confidentiel fourni par le titulaire.

La présente invention se propose de fournir une solution adaptée au problème des chèques volés en vue d'interdire à toute personne non autorisée l'usage d'un carnet de chèques susceptible d'être en sa possession.

Un objectif de l'invention est en particulier d'autoriser la vérification par un bénéficiaire (commerçant...), de la légalité de l'émission d'un chèque bancaire ou postal de type traditionnel sans modification quelconque de ce chèque ou inscription supplémentaire.

Un autre objectif de l'invention est de fournir un système pratiquement inviolable, aussi bien par simulation informatique que par accès physique tendant à décrypter les moyens mis en oeuvre, même pour une personne tel qu'un commerçant ayant le système à sa disposition.

Un autre objectif essentiel de l'invention est de fournir un système de faible coût qui soit compatible

avec les possibilités d'investissement d'un petit commerçant et soit très rapidement rentabilisé par la suppression des pertes dues aux chèques volés.

L'invention vise en particulier à fournir un système dont les moyens essentiels de calcul puissent être supportés par un circuit intégré spécifique du type "prédiffusé" qui permet à partir d'une matrice de transistors disponible sur le marché, d'effectuer des connections spécifiques pour obtenir une fonction globale désirée. On sait que ce type de circuit associe l'avantage d'un coût réduit à celui d'une impossibilité pratique d'accès physique (intégration sur une puce de silicium).

A cet effet, le procédé conforme à l'invention pour vérifier la légalité d'émission de chèques bancaires ou postaux sur lesquels est inscrit un numéro de compte de titulaire à au moins huit chiffres décimaux, consiste :

. à affecter préalablement pour chaque numéro de compte, un code confidentiel décimal à quatre chiffres, en faisant correspondre à l'ensemble antécédent des numéros de compte à au moins huit chiffres, l'ensemble image plus restreint des entiers décimaux de 0 à 9999, ladite correspondance étant une application dans laquelle chaque antécédent possède une seule image laquelle est une fonction logique dudit antécédent,

. et pour chaque vérification d'un chèque, à réaliser la séquence suivante :

(a) à saisir les chiffres du numéro de compte inscrit sur le chèque à vérifier et à engendrer une suite de signaux électriques logiques en nombre au moins égal à 27, représentative en base binaire du numéro de compte saisi,

(b) à réaliser sur ces signaux logiques des opérations logiques correspondant à la fonction logique de l'application précitée, en vue d'engendrer une nouvelle suite de signaux logiques en nombre au plus égal à 14,

(c) à introduire par action du titulaire sur un système d'entrée décimal le code confidentiel à quatre chiffres et à engendrer une suite de signaux logiques en nombre au plus égal à 14, représentative en base binaire

du code confidentiel introduit,

(d) à effectuer une comparaison logique des suites de signaux logiques issus des opérations (b) et (c) , en vue d'engendrer un signal logique de comparaison représentatif de l'identité des deux suites de signaux ou de leur non-identité,

(e) à délivrer ledit signal logique de comparaison vers des moyens avertisseurs, à l'exclusion de la suite de signaux représentative du code confidentiel, en vue d'informer le bénéficiaire du chèque du résultat de la comparaison sans lui fournir le code confidentiel.

Selon une caractéristique de l'invention, les opérations logiques (b) consistent :

(b_1) à répartir les signaux logiques saisis en plusieurs groupes ordonnés de 14 signaux au plus,

(b_2) à effectuer des opérations logiques sur les signaux de chaque groupe,

(b_3) et à effectuer des opérations logiques entre groupes, en vue d'obtenir un groupe résultant formé d'une suite de signaux logiques en nombre au plus égal à 14.

Selon un mode de mise en oeuvre préféré, la répartition (b_1) des signaux logiques saisis est effectué en adressant lesdits signaux dans plusieurs registres selon une table de correspondance aléatoire.

En outre, les opérations logiques (b_2) effectuées sur les signaux de chaque groupe consistent préférentiellement à inverser des signaux selon une table de sélection aléatoire.

De plus, les opérations logiques (b_3) effectuées entre groupe consistent, en particulier, à réaliser des OU exclusifs entre paires de groupes, de façon que chaque groupe intervienne dans au moins une opération de OU exclusif.

Selon une autre caractéristique de l'invention, l'on mémorise au moins un groupe clé constitué par une suite aléatoire de signaux logiques en nombre égal au nombre de signaux de chaque groupe, et l'on effectue les opérations logiques (b_3) en faisant intervenir chaque groupe clé dans au moins une opération de OU exclusif.

Chaque séquence de vérification sus-évoquée

(a, b, c, d, e) est effectuée sur une machine électronique à la disposition du bénéficiaire du chèque (commerçant...), tandis que la phase préalable d'affectation des codes confidentiels à partir des numéros de compte est effectuée au moyen d'une autre machine électronique à la disposition de l'organisme bancaire concerné.

Selon une caractéristique de l'invention, cette phase préalable d'affectation consiste :

(p) à saisir les chiffres du numéro de compte concerné et à engendrer une suite de signaux logiques conformément à l'opération (a),

(q) à réaliser sur ces signaux logiques les opérations logiques (b),

(r) à convertir en base décimale la suite de signaux logiques obtenue,

(s) et à afficher le résultat obtenu constituant le code confidentiel.

La machine électronique à la disposition des commerçants, dite "machine de vérification", comprend conformément à la présente invention un microprocesseur de contrôle et de commande, des moyens de saisie d'un numéro décimal à au moins huit chiffres, des moyens de conversion dudit numéro en base binaire, des moyens de calcul logique pour le traitement dudit numéro en base binaire, un système d'entrée décimal pour l'introduction d'un code confidentiel décimal à 4 chiffres, des moyens de conversion du code en base binaire, des moyens de mémorisation temporaire dudit code en base binaire, des moyens logiques de comparaison du résultat issu des moyens de calcul et du code en base binaire mémorisé et des moyens avertisseurs adaptés pour traduire sous forme sensible le résultat de la comparaison, ladite machine étant caractérisée en ce que les moyens de calcul logique sont adaptés pour faire correspondre à l'ensemble antécédent des numéros en base binaire à au moins 27 bits, l'ensemble image des nombres binaires à au plus 14 bits, inférieurs à 10011100001111, ladite correspondance étant une application dans laquelle chaque antécédent possède une seule image.

Par ailleurs, la machine électronique à la disposition des organismes bancaires, dite "machine d'affectation", comprend, conformément à la présente invention un

microprocesseur de contrôle et de commande, des moyens de saisie d'un numéro décimal à au moins 8 chiffres, des moyens de conversion dudit numéro en base binaire, des moyens de calcul logique pour traiter ledit numéro en base binaire, des moyens de conversion en base décimale du résultat du calcul logique et des moyens d'affichage du résultat décimal, ladite machine étant caractérisée en ce que les moyens de calcul logique sont adaptés pour faire correspondre à l'ensemble antécédent des numéros en base binaire à au moins 27 bits, l'ensemble image des nombres binaires à au plus 14 bits, inférieur à 10011100001111, ladite correspondance étant une application dans laquelle chaque antécédent possède une seule image.

Ainsi, le procédé de l'invention conduit à utiliser le numéro de compte bancaire ou postal du titulaire de sorte qu'aucune modification des chèques n'est exigée puisque ce numéro (de 8 à 12 chiffres) est déjà inscrit de façon apparente sur chaque chèque ; la saisie des chiffres dudit numéro de compte est effectuée, lors de la vérification du chèque, soit par lecture directe sur le chèque au moyen d'un lecteur approprié (lecteur optique en particulier à transfert de charge, lecteur magnétique,...), soit par introduction sur un clavier par le titulaire du compte ou par le bénéficiaire du chèque.

A partir de ce numéro converti en binaire, le code confidentiel est calculé par la fonction logique évoquée qui permet de faire correspondre, par un calcul simple, à l'ensemble des numéros de compte, un ensemble plus restreint de codes confidentiels à 4 chiffres décimaux (facilement mémorisables par le titulaire du compte) ; comme on le comprendra mieux plus loin, la correspondance prévue conserve une répartition des codes confidentiels identique à celle des numéros de compte : en d'autres termes, pour des numéros de compte ayant une probabilité identique d'apparition, on obtient des codes confidentiels ayant approximativement une même probabilité d'apparition (on évite ainsi que l'ensemble des numéros de compte se traduise par un sous-ensemble restreint parmi les 9999 premiers nombres décimaux).

Malgré la simplicité des opérations logiques qu'elle implique, la correspondance prévue dans l'invention est pratiquement inviolable par déduction mathématique ou

simulation informatique pour les raisons expliquées ci-après.

En premier lieu, la correspondance entre numéros de compte (nombre à au moins 8 chiffres décimaux et généralement à 11 ou 12 chiffres) et codes confidentiels (nombre à 4 chiffres décimaux) s'effectue avec une perte énorme d'informations (dans le cas d'un numéro à 12 chiffres, une donnée sur 10^8 est conservée) ; cette caractéristique combinée à la nature de la loi de correspondance prévue dans l'invention rend pratiquement impossible une déduction logique d'un code confidentiel à partir d'un numéro de compte. Cette loi de correspondance se traduit par des opérations de répartition (b_1), d'inversion (b_2) ou de combinaison de groupes (b_3) qui s'effectuent selon des tables aléatoires combinées, rompant le caractère de pure logique de la correspondance. Il est à noter que ces tables ne sont pas lisibles car elles ne sont utilisées que pour fournir des résultats temporaires non accessibles à l'utilisateur.

De plus, l'utilisation d'une ou plusieurs clés aléatoires avec lesquelles sont effectuées les opérations de combinaison de groupe (b_3) contribue à supprimer toute logique de correspondance.

Par ailleurs, la simplicité des opérations impliquées et la faible capacité des tables aléatoires nécessaires permettent d'assurer la mise en oeuvre du procédé avec des circuits logiques de structures simples et des moyens de mémorisation de faibles dimensions. En particulier, les moyens de calcul de même que les moyens logiques de comparaison peuvent être réalisés de façon connue en soi sur un circuit intégré spécifique du type "prédiffusé", les tables aléatoires étant réalisées par des connections aléatoires. Cette conception en prédiffusé interdit, d'une part, toute analyse physique des circuits puisque ceux-ci se traduisent sur une puce de silicium pratiquement inpénétrable, d'une part, une lecture des logiciels de calcul puisque ceux-ci sont réalisés par des jonctions physiques entre transistors et non par des informations programmées (lesquelles peuvent toujours être lues par des moyens informatiques).

L'invention sera mieux comprise à la lecture de la description qui suit et à l'examen des dessins

annexés ; sur ces dessins :

- la figure 1 est une vue en perspective d'une machine de vérification de chèque, destinée à être mise à la disposition d'un commerçant,

- la figure 2 est un schéma synoptique des moyens électroniques de ladite machine,

- les figures 3a et 3b sont des logigrammes qui illustrent les traitements logiciels spécifiques se déroulant dans la machine,

- la figure 4 est un schéma synoptique d'un mode de réalisation des moyens de calcul et moyens de comparaison de ladite machine,

- les figures 5, 6 et 7 représentent des exemples de circuits cablés formant ces moyens de calcul,

- les figures 8a, 8b et 8c donnent des exemples de tables aléatoires pré-établies,

- la figure 9 illustre un exemple d'application du procédé de l'invention,

- la figure 10 est un schéma synoptique d'une machine d'affectation de codes confidentiels, destinée à être mise à la disposition d'un organisme bancaire.

La machine de vérification schématisée aux figures 1 et 2 comprend une partie électronique cablée et une partie programmée.

La partie programmée est composée :

. d'un microprocesseur µP de type "mono-chip" optimisé pour des applications temps-réel,

. d'une mémoire morte PROM qui contient le logiciel de traitement,

. et d'une mémoire vive RAM qui reçoit des données temporaires.

La partie cablée comprend un clavier décimal CL à la disposition du client, associé à des moyens de conversion décimal/binaire CV. Ce clavier permettra au client d'entrer son code confidentiel.

En outre, un lecteur magnétique MG assure l'acquisition automatique de 12 chiffres représentatifs du numéro de compte imprimé à l'encre magnétique sur chaque

chèque. Ce lecteur, de type connu en soi, possède des moyens de traitement qui permettent à partir de ces chiffres, de délivrer des signaux binaires représentatifs desdits chiffres ; ces signaux sont analysés par le microprocesseur qui délivre vers sa mémoire RAM les 42 bits correspondant en binaire aux 12 chiffres décimaux du numéro de compte.

Ces 42 bits sont adressés à un circuit intégré prédiffusé qui comprend des moyens de calcul CAL et des moyens de comparaison COMP. Un mode de réalisation de ces moyens est décrit plus loin.

La machine comprend également un afficheur AFF à cristaux liquides à 12 caractères en vue d'afficher soit le numéro de compte chèque après saisie magnétique, soit des messages traduisant les résultats de calcul. Cet afficheur est destiné au commerçant. Cet afficheur est associé à une sonnerie SON destinée à avertir le commerçant de la correspondance (ou non) entre numéro de compte et code confidentiel.

En outre, quatre voyants lumineux LA_1, LA_2, LA_3, LA_4 portant quatre instructions pour le client, sont disposés au-dessus du clavier CL :

- LA_1 : "entrez votre code confidentiel",
- LA_2 : "recommencez s'il vous plait",
- LA_3 : "votre chèque est accepté",
- LA_4 : "votre chèque est refusé".

Ces voyants sont commandés par le microprocesseur μP par l'entremise d'une interface de commande ILA soit après lecture magnétique du numéro de compte, soit en fonction des résultats issus des moyens de comparaison COMP.

De façon classique, les signaux de commande générés par le microprocesseur sont délivrés à chaque unité par l'intermédiaire d'une interface combinatoire IC.

Dans le mode de réalisation représenté à la figure 1, le clavier CL et les voyants $LA_1 \ldots LA_4$ sont portés par un support manipulable par le client ; ce support est relié par un cable souple à un boîtier qui comprend tous les autres moyens et est appelé à être disposé en face du commerçant, en général près de sa caisse.

La gestion de la machine par le microprocesseur μP est illustrée aux figures 3a et 3b (par "instruc-

tion", on entend ci-après aussi bien des instructions élémentaires qu'une série d'instructions réalisant une action).

Lorsque la machine est mise sous tension, une étape préalable d'initialisation des mémoires vives est réalisée ; en particulier le nombre d'erreurs déjà commises (non correspondance entre le code confidentiel et le numéro de compte) est remise à zéro dans la zone "RAM" du microprocesseur.

Une instruction de sortie commande ensuite l'affichage sur l'afficheur AFF (à la disposition du commerçant) du message suivant : "LIRE CHEQUE". Le commerçant sait alors qu'il doit introduire le chèque dans le lecteur magnétique MG.

Un test de fin d'acquisition de numéro de compte de chèque est ensuite pratiqué.

Après acquisition, le voyant LA_1 est validé par l'instruction suivante. Ce voyant porte la mention : "Rentrez votre code confidentiel", de façon que le client frappe son code sur le clavier CL. Il est à noter que ce code ne devient apparent à aucun moment et n'est pas communiqué au commerçant.

Un test de fin d'acquisition du code confidentiel est ensuite pratiqué.

Une instruction de conversion commande ensuite la conversion en binaire du numéro lu par le lecteur MG. Une autre instruction assure la même commande pour le code confidentiel.

Les deux instructions qui suivent commandent l'intervention des moyens de calcul CAL du circuit prédiffusé. La procédure détaillée de déroulement des calculs est décrite plus loin, en relation avec la structure de ces moyens de calcul.

Un test de résultat de comparaison est ensuite réalisé. En cas d'erreur, on se reporte à la procédure erreur décrite plus loin en référence à la figure 3b. En cas de correspondance, on valide le voyant LA_3 qui indique au client que son chèque est accepté, on affiche sur l'afficheur AFF "BON" et on valide une sonnerie significative du bon résultat (par exemple un "bip" léger).

La procédure générale est terminé et le

logigramme se reboucle sur lui-même pour la vérification suivante.

La procédure d'erreur est illustrée à la figure 3b. En cas de comparaison détectant une non correspondance entre numéro de chèque et code confidentiel, une instruction valide le voyant LA_3 "Recommencez s'il vous plaît".

Une instruction de décompte du nombre d'erreurs est fournie au microprocesseur.

Un test sur le décompte présent est réalisé. Si ce décompte est inférieur à 4, une instruction d'affichage de la mention "Tentative n° i" assure l'inscription de cette mention sur l'afficheur AFF.

Les instructions suivantes initialisent la tentative suivante et renvoient à l'étape "recommencez" de la procédure générale.

Si le décompte est supérieur ou égal à 4, une instruction assure l'affichage de la mention "MAUVAIS" sur l'afficheur AFF ; une instruction valide la sonnerie SON pour fournir la sonorité correspondant à un échec (par exemple : série de bips aigus).

La figure 4 est un schéma synoptique des moyens électroniques composant le prédiffusé : moyens de calcul CAL et moyens de comparaison COMP.

Les 42 bits représentatifs du numéro de compte en base binaire sont adressés de la mémoire "RAM" associée au microprocesseur μP vers les moyens de calcul CAL.

Ces 42 bits sont répartis en trois groupes par des moyens logiques de répartition LR dans trois registres R_1, R_2 et R_3 ayant une capacité de 14 bits chacun ; cette répartition est faite selon une table de correspondance aléatoire MR qui fournit pour chaque bit d'entrée, en fonction de sa position temporelle et/ou spatiale, la place où il doit être stocké dans les registres R_1, R_2, R_3 ; cette table contient 42 correspondances. Il est à noter que ces moyens logiques LR et cette table MR sont, dans le cas du prédiffusé, réalisés par l'ensemble des connections entre les entrées et les registres.

La figure 5 illustre un exemple d'un tel circuit cablé, réalisant les fonctions LR et MR.

Les 14 bits stockés dans chaque registre R_1, R_2, R_3 sont ensuite inversés selon une table de sélection aléatoire MI_1, MI_2, MI_3, par des moyens d'inversion LI_1, LI_2, LI_3 ; chaque table de sélection contient 14 états ; le résultat est stocké dans des registres temporaires RT_1, RT_2, RT_3. Comme précédemment, les tables MI_1, MI_2 et MI_3 sont dans le cas du prédiffusé, réalisées par connections ; les registres R_1, R_2, R_3 possèdent une sortie directe et une sortie complémentée et jouent le rôle des moyens d'inversion, cependant que l'ensemble des connections entre ces sorties et les registres temporaires RT_1, RT_2 et RT_3 remplissent la fonction de tables aléatoires de sélection.

La figure 6 illustre un exemple d'un tel circuit d'inversion cablé. Les 14 cellules du registre R_1 (symbolisées à cette figure) reçoivent les bits répartis par LR ; les fonctions LI_1 et MI_1 sont réalisées par la connection de la sortie directe ou complémentaire de chacune de ces cellules avec l'entrée du registre RT_1.

Les sorties des registres temporaires RT_1, RT_2 et RT_3 sont reliées à des opérateurs OU exclusifs L_1 et L_2 ; le résultat de ces opérations est délivré à un autre opérateur OU exclusif L_3 qui reçoit par ailleurs le contenu d'un registre RC. Ce registre contient un groupe clé de 14 bits.

Dans le cas du prédiffusé, ce registre RC est réalisé par connections au niveau 0 ou au niveau 1 des entrées correspondantes de l'opérateur L_3.

Le résultat issu de l'opérateur L_3 est mémorisé dans un registre RS de capacité égale à 14 bits.

Ce résultat est ensuite comparé par un opérateur de comparaison LC au contenu d'une mémoire MC dans laquelle est inscrit l'équivalent binaire de 9999. Cet opérateur LC commande un opérateur de complémentation LP. Si le groupe de bits résultat stocké dans RS est supérieur à MC, l'opérateur LP réalise une inversion de chaque bit de RS de façon à ramener le nombre à une valeur inférieure à 9999 ; dans le cas contraire, l'opérateur assure le passage direct des bits.

Dans le cas du prédiffusé, la mémorisation MC de l'équivalent binaire de 9999 est réalisée par connections.

La figure 7 illustre un tel circuit cablé.

Un ensemble d'opérateurs OU et ET est connecté aux sorties directes ou complémentées du registre RS, de façon à opérer un traitement de bits équivalent à la comparaison précitée.

Les 14 bits issus de l'opérateur LP constituent le code confidentiel calculé par la machine à partir du numéro de compte saisi magnétiquement.

Ce code calculé est comparé dans le comparateur COMP au code confidentiel entré par le client, après conversion en binaire ; ce dernier code confidentiel inscrit dans la mémoire RAM associée au microprocesseur est stocké temporairement dans un registre à 14 bits RCC et la comparaison est effectuée par un opérateur OU exclusif LCC. En cas d'égalité, le groupe de 14 zéros obtenu est traduit dans un opérateur OU LCE par un bit unique égal à zéro. En cas d'inégalité, un bit au moins est 1 à la sortie de LCC et l'opérateur LCE fournit un bit unique égal à 1.

Le bit issu de LCE est le résultat de la comparaison et provoque les validations déjà évoquées.

A titre d'illustration, les figures 8a, 8b et 8c donnent un exemple de tables aléatoires de répartition et d'inversion et un exemple de groupe clé ; la figure 9 montre les traitements assurés par les moyens de calcul CAL d'après ces tables et groupe clé dans le cas du nombre binaire correspondant au numéro de compte 000688971808 (le code confidentiel correspondant en l'exemple est 2245, une fois traduit en décimal).

Les moyens de calcul ci-dessus décrits permettent d'obtenir une infinité de corrélations possibles en fonction des tables (constituées par des connections dans le cas du prédiffusé). Ainsi, ces moyens de calcul combinent une simplicité structurelle compatible avec une réalisation en prédiffusé et un nombre possible de corrélations pratiquement infini ; la réalisation en prédiffusé écarte toute possibilité d'analyse physique des circuits ; de plus le code confidentiel calculé n'apparaît pas en dehors du prédiffusé, ce qui rend extrêmement difficile une analyse informatique du système. En outre, la corrélation fournie par ces moyens de calcul entre numéro de compte et code confidentiel assure une répartition des codes confidentiels à peu près similaire à celle des numéros de compte (sans concentration sur un sous-ensemble res-

treint des 9999 premiers décimaux).

La figure 9 est un schéma synoptique d'une machine d'affectation de code à partir d'un numéro de compte. Cette machine permet à l'organisme bancaire de fournir à chaque titulaire de compte son code confidentiel.

Cette machine possède une structure et un fonctionnement analogues à la précédente. Toutefois, elle est contenue dans un seul boîtier et ne comporte pas de moyens de comparaison COMP, de lecteur magnétique MG et de voyants LA ; les moyens de calcul CAL peuvent être soit cablés en prédiffusé ou en logique standard, soit réalisés par logiciel (le caractère d'inviolabilité est moins essentiel puisque cette machine n'est pas accessible au public). La procédure est analogue à la précédente, mais dans ce cas, le numéro de code est saisi par le clavier CL et le code confidentiel résultat du calcul vient s'inscrire sur l'afficheur AFF.

REVENDICATIONS

1/ - Procédé de vérification de la légalité d'émission de chèques bancaires ou postaux, en vue de permettre aux bénéficiaires de détecter les chèques volés, lesdits chèques bancaires ou postaux étant du type sur lequel est inscrit un numéro de compte de titulaire à au moins huit chiffres décimaux, ledit procédé étant caractérisé en ce qu'il consiste :

. à affecter préalablement pour chaque numéro de compte, un code confidentiel décimal à quatre chiffres, en faisant correspondre à l'ensemble antécédent des numéros de compte à au moins huit chiffres, l'ensemble image plus restreint des entiers décimaux de 0 à 9999, ladite correspondance étant une application dans laquelle chaque antécédent possède une seule image laquelle est une fonction logique dudit antécédent /

. et pour chaque vérification d'un chèque, à réaliser la séquence suivante :

(a) à saisir les chiffres du numéro de compte inscrit sur le chèque à vérifier et à engendrer une suite de signaux électriques logiques en nombre au moins égal à 27, représentative en base binaire du numéro de compte saisi,

(b) à réaliser sur ces signaux logiques des opérations logiques correspondant à la fonction logique de l'application précitée, en vue d'engendrer une nouvelle suite de signaux logiques en nombre au plus égal à 14,

(c) à introduire par action du titulaire sur un système d'entrée le code confidentiel décimal à quatre chiffres et à engendrer une suite de signaux logiques en nombre au plus égal à 14, représentative en base binaire du code confidentiel introduit,

(d) à effectuer une comparaison logique des suites de signaux logiques issus des opérations (b) et (c), en vue d'engendrer un signal logique de comparaison représentatif de l'identité des deux suites de signaux ou de leur non-identité,

(e) à délivrer ledit signal logique de comparaison vers des moyens avertisseurs, à l'exclusion de la suite de signaux représentative du code confidentiel, en vue d'informer le bénéficiaire du chèque du résultat de la compa-

raison sans lui fournir le code confidentiel.

2/ - Procédé selon la revendication 1, caractérisé en ce que les opérations logiques (b) consistent :

(b_1) à répartir les signaux logiques saisis en plusieurs groupes ordonnés de 14 signaux au plus,

(b_2) à effectuer des opérations logiques sur les signaux de chaque groupe,

(b_3) et à effectuer des opérations logiques entre groupes, en vue d'obtenir un groupe résultant formé d'une suite de signaux logiques en nombre au plus égal à 14.

3/ - Procédé selon la revendication 2, caractérisé en ce que la répartition (b_1) des signaux logiques saisis est effectuée en adressant lesdits signaux dans plusieurs registres selon une table de correspondance aléatoire.

4/ - Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que les opérations logiques (b_2) effectuées sur les signaux de chaque groupe consistent à inverser des signaux selon une table de sélection aléatoire.

5/ - Procédé selon la revendication 4, caractérisé en ce que l'on effectue des opérations logiques d'inversion (b_2) sur chacun des groupes selon des tables de sélection différentes.

6/ - Procédé selon l'une des revendications 2, 3, 4 ou 5, caractérisé en ce que les opérations logiques (b_3) effectuées entre groupe consistent à réaliser des OU exclusifs entre paires de groupes, de façon que chaque groupe intervienne dans au moins une opération de OU exclusif.

7/ - Procédé selon la revendication 6, caractérisé en ce que l'on mémorise au moins un groupe clé constitué par une suite aléatoire de signaux logiques en nombre égal au nombre de signaux de chaque groupe, et l'on effectue les opérations logiques (b_3) en faisant intervenir chaque groupe clé dans au moins une opération de OU exclusif.

8/ - Procédé selon l'une des revendications 2, 3, 4, 5, 6 ou 7, caractérisé en ce que la répartition (b_1) des signaux saisis est opérée en trois groupes dans trois registres.

9/ - Procédé selon l'une des revendications

2, 3, 4, 5, 6, 7 ou 8, destiné au traitement de chèque du type sur lequel est inscrit un numéro de compte à 11 ou 12 chiffres décimaux, caractérisé en ce que :

(a) l'on saisit les 11 ou 12 chiffres du numéro de compte et l'on engendre une suite de signaux logiques en nombre égal à 42,

(b) l'on répartit ces signaux logiques en 3 groupes de 14 signaux et l'on effectue sur ces groupes ou entre ces groupes les opérations d'inversion (b_2) ou de OU exclusif (b_3), en vue d'engendrer un groupe résultant constitué par une suite de 14 signaux logiques.

10/ - Procédé selon la revendication 9, caractérisé en ce que les opérations logiques (b) sont complétées par les opérations suivantes (b_4, b_5, b_6) effectuées sur la suite des 14 signaux logiques obtenues :

(b_4) comparaison de la suite obtenue au nombre binaire 10011100001111 correspondant à 9999,

(b_5) en cas de supériorité de ladite suite, complémentation de cette suite,

(b_6) en cas d'infériorité ou d'égalité, validation de cette suite telle quelle.

11/ - Procédé selon l'une des revendications précédentes, caractérisé en ce que la comparaison logique (d) des suites de signaux issus des opérations (b) et (c) est opérée en effectuant un OU exclusif entre ces deux suites, puis un OU logique de tous les signaux résultants en vue d'obtenir le signal logique de comparaison.

12/ - Procédé selon l'une des revendications précédentes, caractérisé en ce que, à l'issue de l'opération de saisie (a), on visualise les chiffres décimaux du numéro de compte et l'on valide le système d'entrée décimal permettant l'introduction (c) du code confidentiel.

13/ - Procédé selon l'une des revendications précédentes, caractérisé en ce que la phase préalable d'affectation du code confidentiel correspondant à chaque numéro de compte consiste :

(p) à saisir les chiffres du numéro concerné et à engendrer une suite de signaux logiques conformément à l'opération (a).

(q) à réaliser sur ces signaux logiques les opérations logiques (b),

(r) à convertir en base décimale la suite de signaux logiques obtenue,

(s) et à afficher le résultat obtenu constituant le code confidentiel.

14/ - Procédé selon la revendication 13, caractérisé en ce que la phase préalable d'affectation (p, q, r, s) est effectuée au moyen d'une première machine électronique à la disposition d'un organisme bancaire, tandis que chaque séquence de vérification (a, b, c, d, e) est effectuée sur une seconde machine électronique à la disposition du bénéficiaire du chèque.

15/ - Machine électronique de vérification d'un chèque, en vue de la réalisation des séquences de vérification conformes au procédé selon l'une des revendications précédentes, comprenant un microprocesseur (µP) de contrôle et commande, des moyens de saisie d'un numéro décimal à au moins huit chiffres (MG), des moyens de conversion dudit numéro en base binaire (µP), des moyens de calcul logique pour le traitement dudit numéro en base binaire (CAL), un système d'entrée décimal (CL) pour l'introduction d'un code confidentiel décimal à 4 chiffres, des moyens de conversion du code en base binaire (CV), des moyens de mémorisation temporaire dudit code en base binaire (RAM), des moyens logiques (COMP) de comparaison du résultat issu des moyens de calcul et du code en base binaire mémorisé, et des moyens avertisseurs (AFF ; SON ; LA_3, LA_4) adaptés pour traduire sous forme sensible le résultat de la comparaison, ladite machine étant caractérisée en ce que les moyens de calcul logique (CAL) sont adaptés pour faire correspondre à l'ensemble antécédent des numéros en base binaire à au moins 27 bits, l'ensemble image des nombres binaires à au plus 14 bits, inférieurs à 10011100001111, ladite correspondance étant une application dans laquelle chaque antécédent possède une seule image.

16/ - Machine selon la revendication 15, caractérisée en ce que les moyens logiques de comparaison (COMP) comprennent :

. un opérateur OU exclusif (LCC) agencé

pour recevoir le résultat issu des moyens de calcul (CAL) et le code binaire contenu dans les moyens de mémorisation (RAM),

. un opérateur OU (LCE) agencé pour opérer sur chaque bit issu de l'opérateur (LCC) en vue de délivrer un signal logique de commande des moyens avertisseurs.

17/ - Machine électronique pour affecter à un numéro de compte un code confidentiel, comprenant un microprocesseur (μP) de contrôle et commande, des moyens de saisie d'un numéro décimal à au moins 8 chiffres (CL), des moyens de conversion dudit numéro en base binaire (CV), des moyens de calcul logique (CAL) pour traiter ledit numéro en base binaire, des moyens de conversion en base décimale du résultat du calcul logique (μP) et des moyens d'affichage du résultat décimal (AFF), ladite machine étant caractérisée en ce que les moyens de calcul logique (CAL) sont adaptés pour faire correspondre à l'ensemble antécédent des numéros en base binaire à au moins 27 bits, l'ensemble image des nombres binaires à au plus 14 bits, inférieurs à 10011100001111, ladite correspondance étant une application dans laquelle chaque antécédent possède une seule image.

18/ - Machine selon la revendication 15 ou la revendication 17, caractérisée en ce que ses moyens de calcul logique (CAL) comprennent plusieurs registres de mémoire vive (R_1, R_2, R_3) pour mémoriser plusieurs groupes de bits, une table de correspondance aléatoire (MR), des moyens logiques (LR) de répartition dans les registres selon la table de correspondance (MR), au moins une table de sélection (MI_1, MI_2, MI_3) de bits à inverser, des moyens d'inversion (LI_1, LI_2, LI_3) de bits à inverser selon les tables de sélection, des opérateurs logiques (L_1, L_2, L_3) agencés pour combiner les bits issus des moyens d'inversion (LI) et un registre de mémoire vive (RS) pour mémoriser le résultat issu desdits opérateurs.

19/ - Machine selon la revendication 18, caractérisée en ce que les moyens de calcul (CAL) comprennent en outre au moins un registre (RC) pour mémoriser un groupe clé, les opérateurs logiques (L_1, L_2, L_3) étant agencés pour combiner les bits dudit registre et ceux des registres de mémoire vive (R_1, R_2, R_3) précités.

20/ - Machine selon la revendication 19,

caractérisée en ce que les moyens de calcul (CAL) comprennent :

. trois registres de mémoire vive (R_1, R_2, R_3) chacun de capacité égale à 14 bits,

. une table de correspondance aléatoire (MR) contenant 42 correspondances,

. trois tables de sélection aléatoires différentes (MI_1, MI_2, MI_3), contenant chacune 14 états,

. un registre de mémoire vive (RS) de capacité égale à 14 bits pour mémoriser le résultat.

21/ - Machine selon l'une des revendications 19 ou 20, caractérisée en ce que les moyens de calcul (CAL) comprennent au moins trois opérateurs logiques (L_1, L_2, L_3) constitués par des OU exclusifs.

22/ - Machine selon l'une des revendications 18, 19, 20 ou 21, caractérisée en ce que les moyens de calcul (CAL) comprennent :

. une mémoire (MC) pour la mémorisation d'un nombre binaire à 14 bits,

. un opérateur (LC) de comparaison du résultat inscrit dans le registre de mémoire vive (RS) avec le nombre binaire mémorisé dans la mémoire (MC) précitée.

. un opérateur de complémentation (LP) commandé par l'opérateur de comparaison (LC) en fonction du résultat de la comparaison.

23/ - Machine selon l'une des revendications 15 à 22, dans laquelle les moyens de calcul logique (CAL) et les moyens logiques de comparaison (COMP) sont réalisés sur un circuit intégré spécifique du type "prédiffusé", les tables aléatoires étant réalisées par des connections aléatoires.

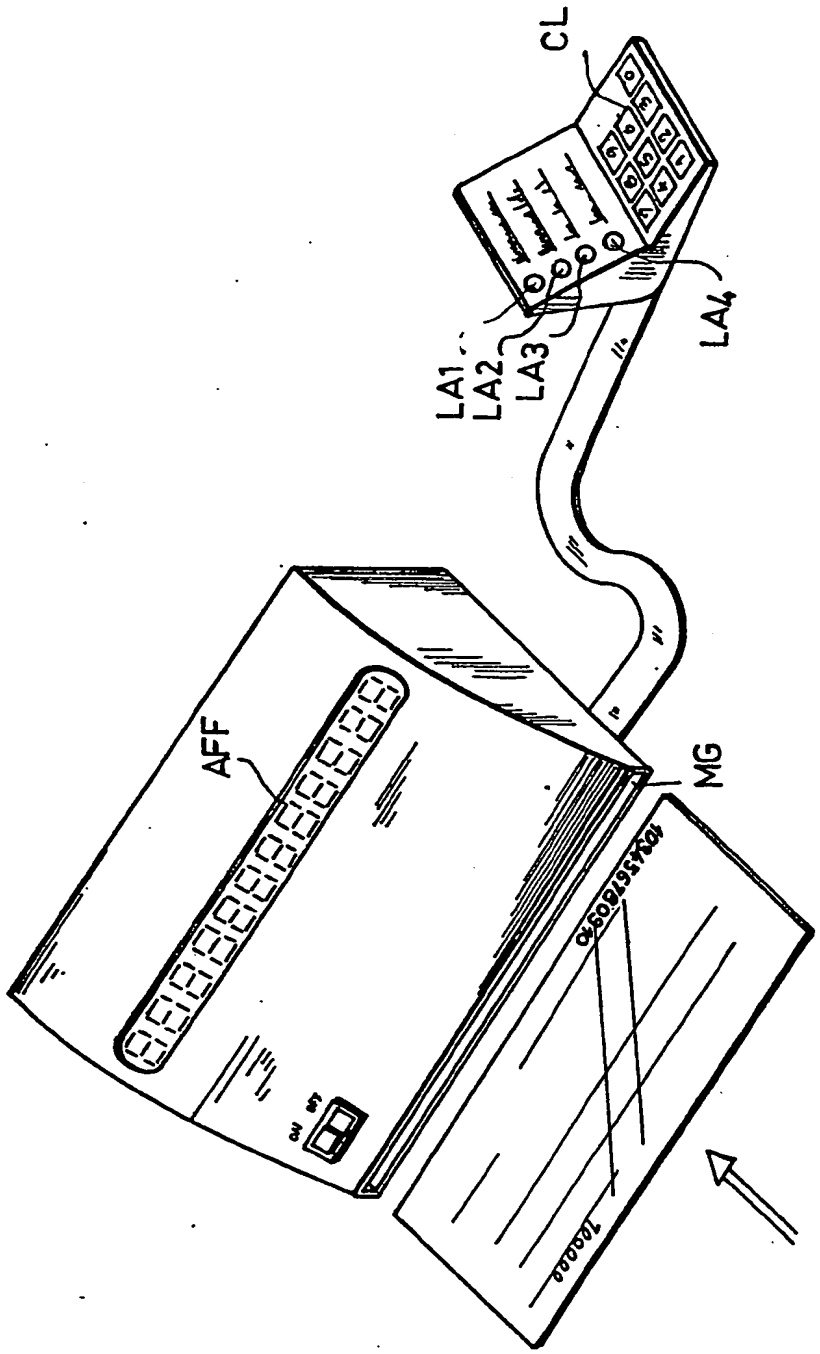


Fig. 1

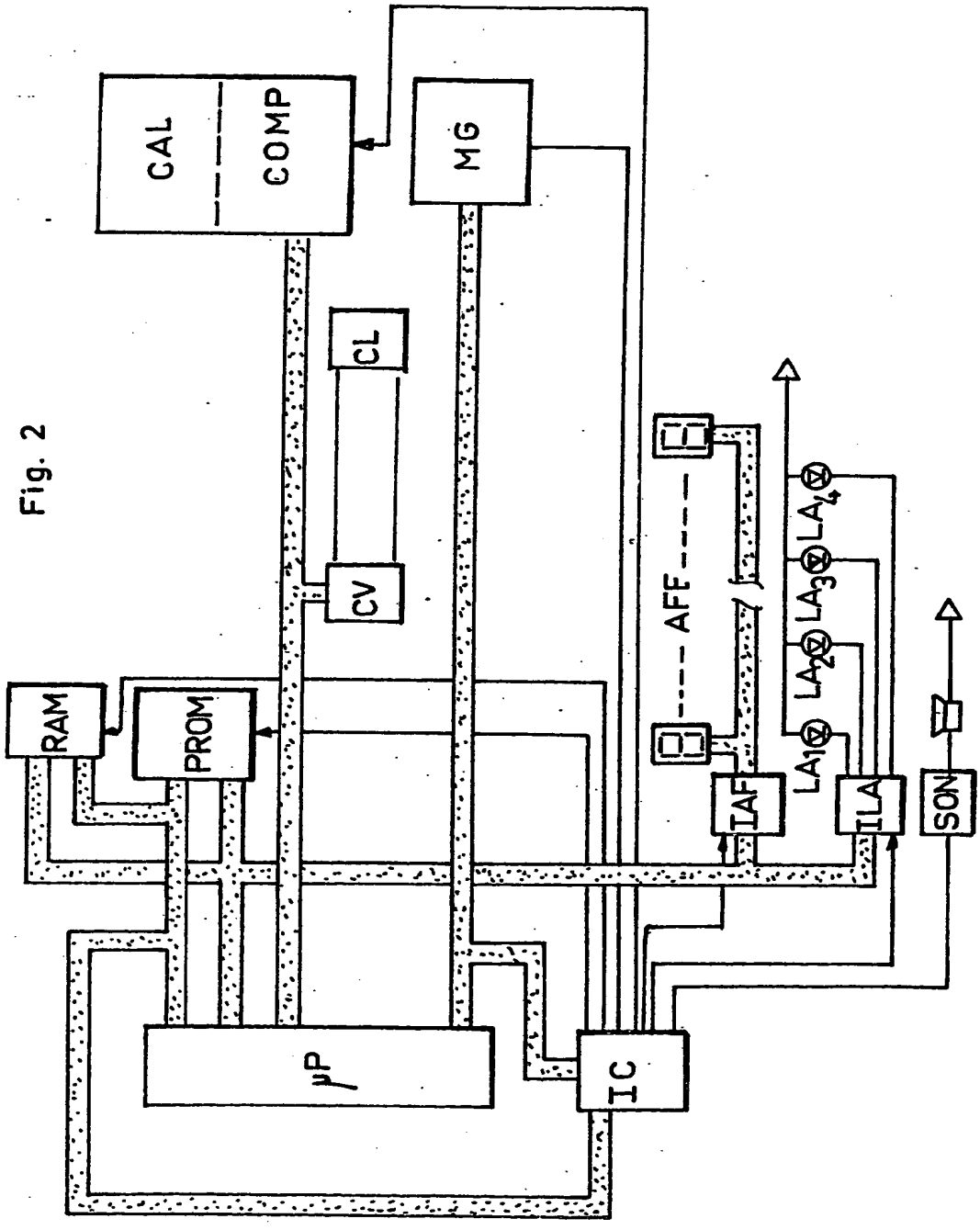


Fig. 2

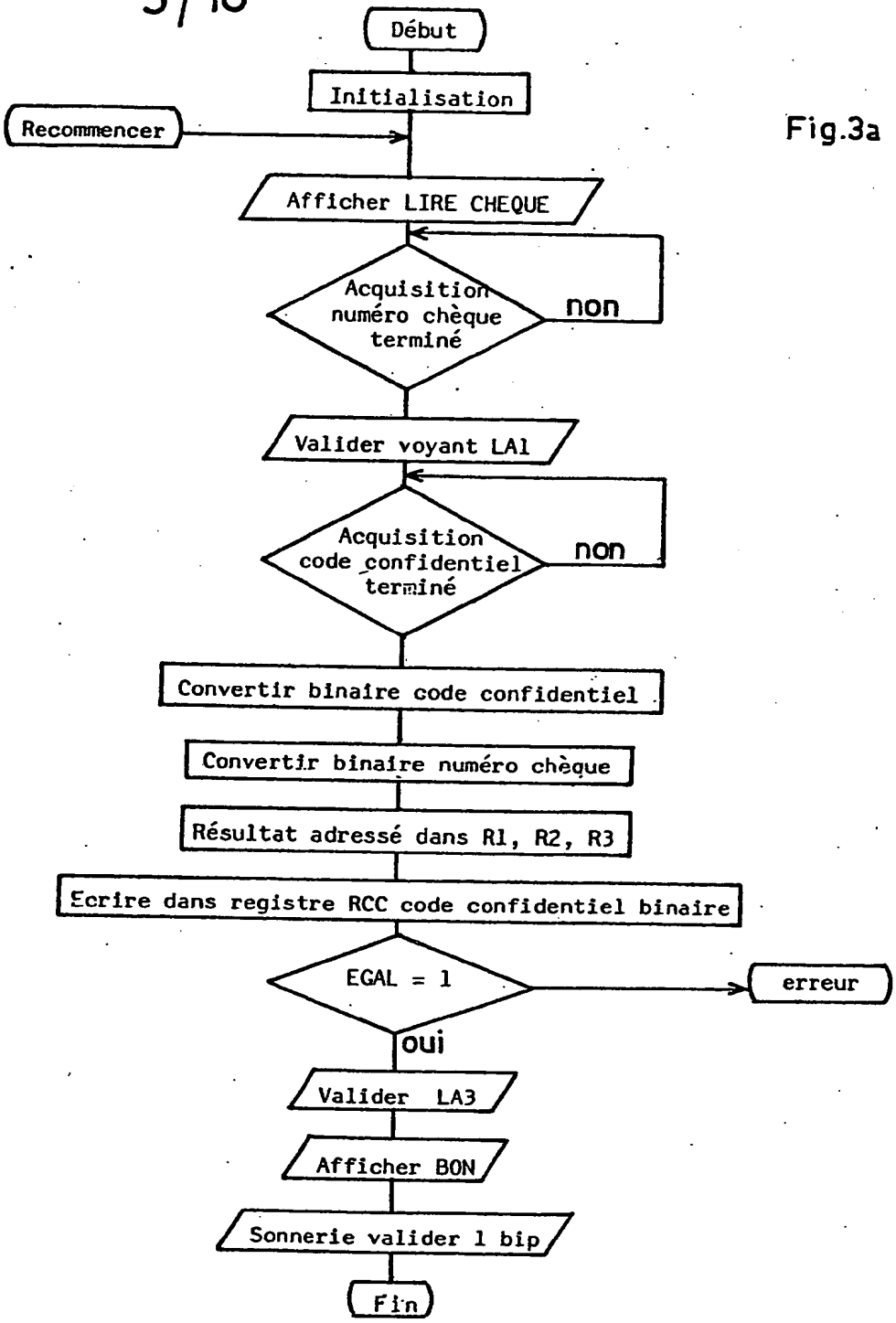


Fig.3a

Fig. 3b

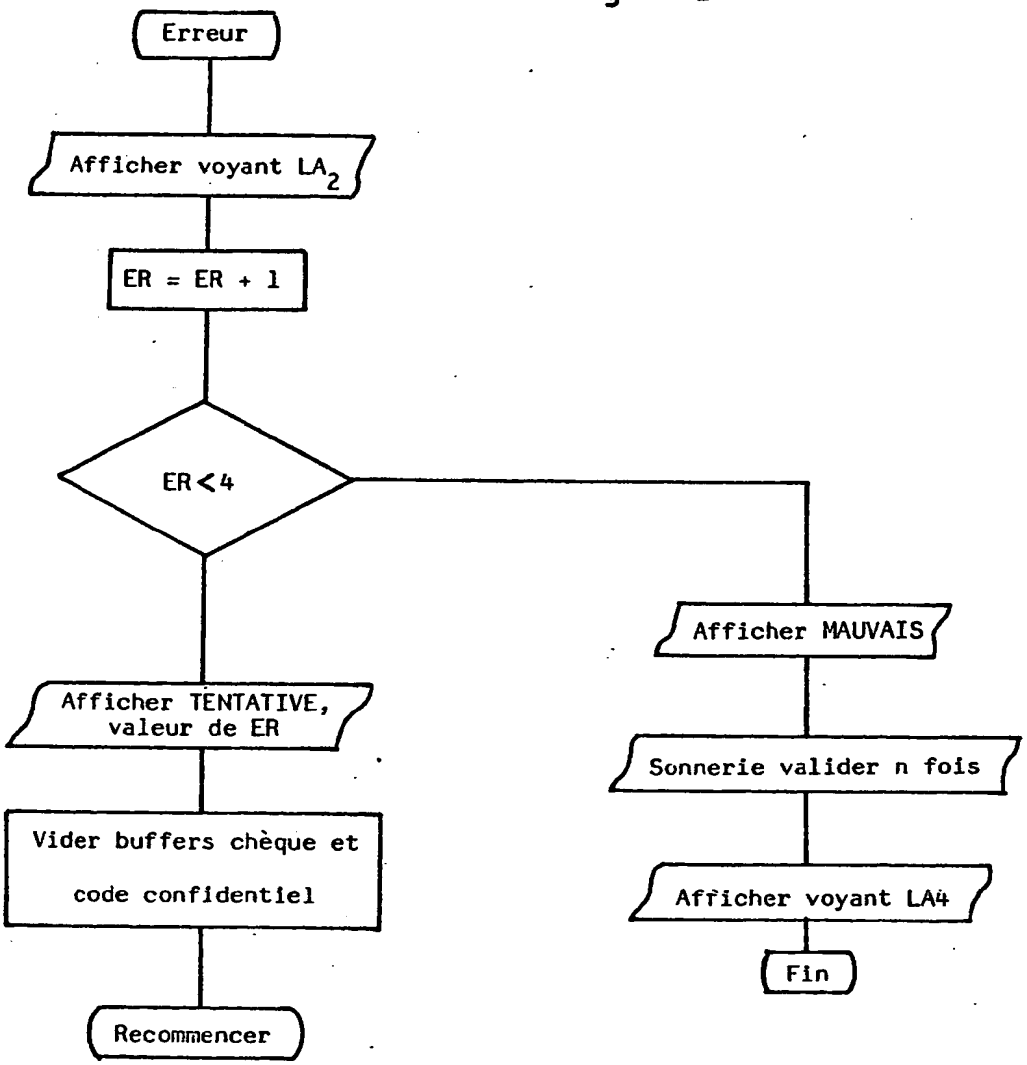
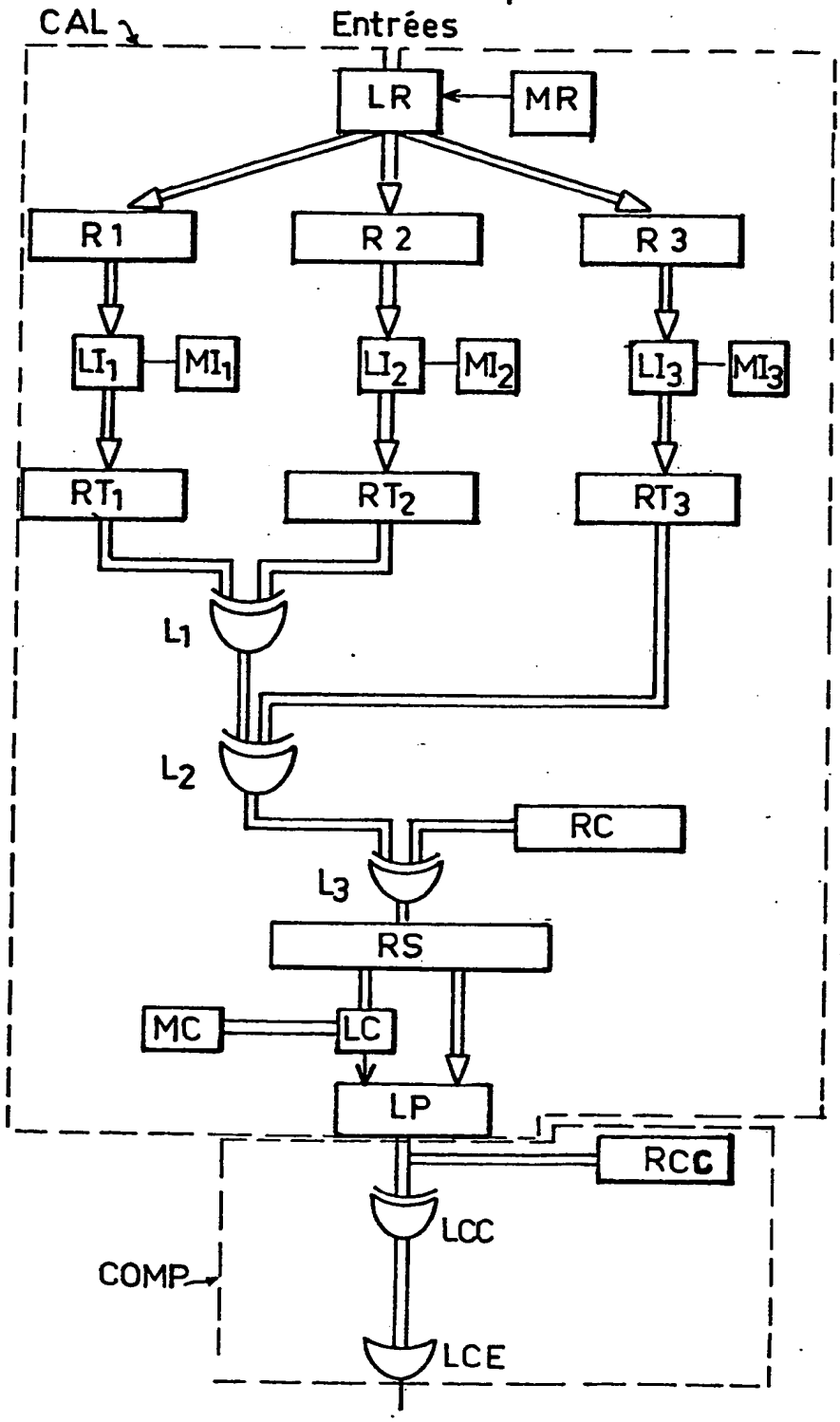


Fig. 4



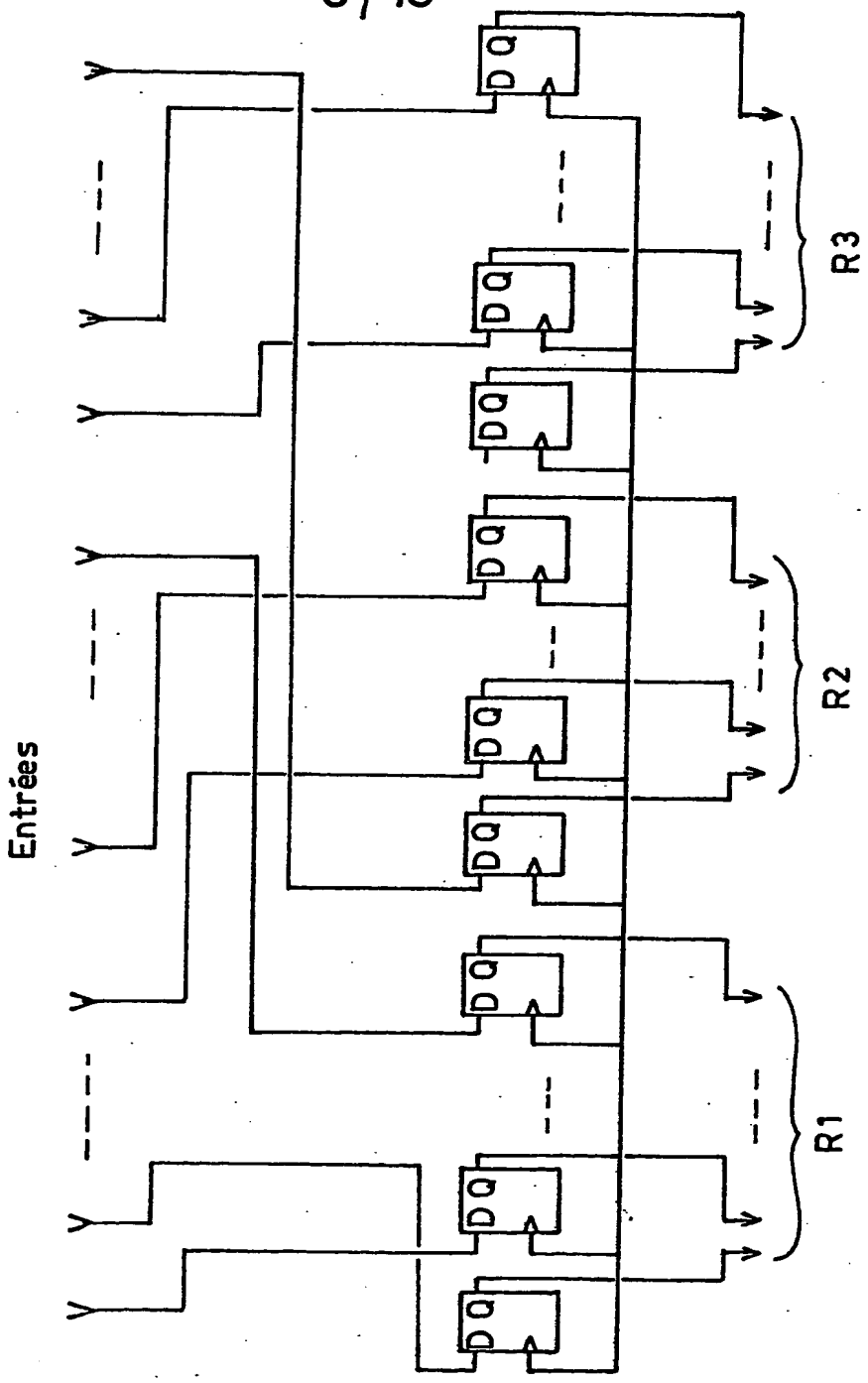


Fig. 5

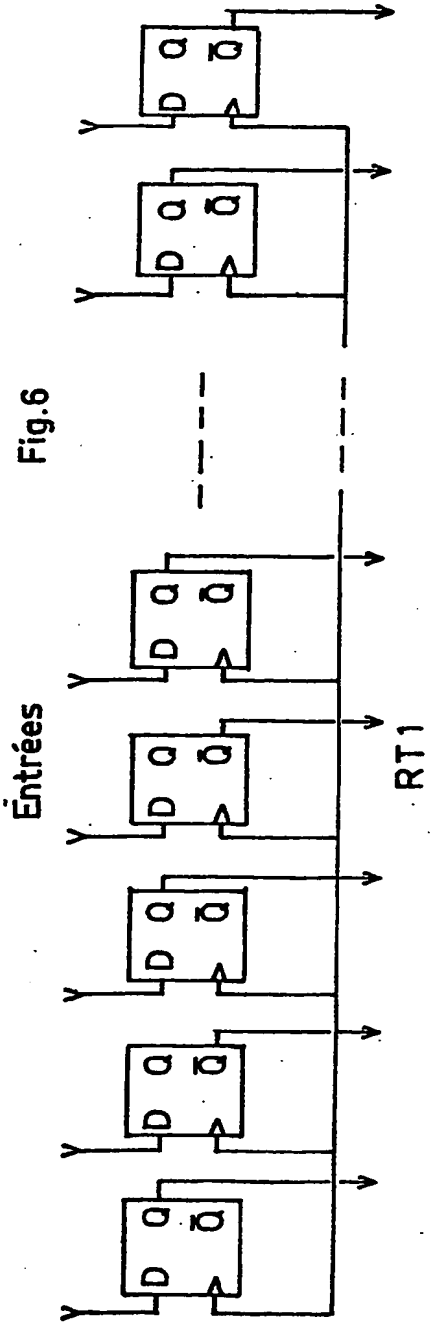


Fig.6

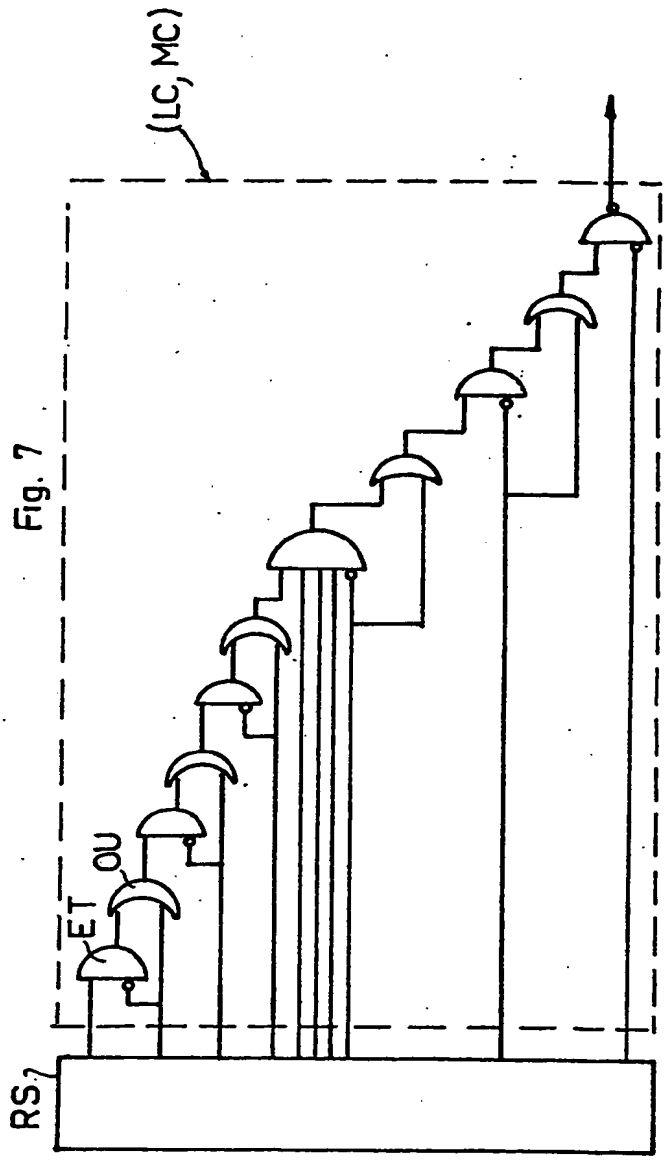


Fig. 7

Fig.8a

MR	R1, R2, R3
1	2 - R2
2	4 - R2
3	5 - R3
4	7 - R3
5	13 - R1
6	14 - R1
7	1 - R2
8	8 - R2
9	11 - R2
10	9 - R1
11	12 - R3
12	10 - R3
13	3 - R3
14	6 - R2
15	2 - R3
16	4 - R3
17	5 - R1
18	7 - R1
19	13 - R2
20	14 - R2
21	1 - R3
22	8 - R3
23	11 - R3
24	9 - R2
25	12 - R1
26	10 - R1
27	3 - R1
28	6 - R3
29	2 - R1
30	4 - R1
31	5 - R2
32	7 - R2
33	13 - R3
34	14 - R3
35	1 - R1
36	8 - R1
37	11 - R1
38	9 - R3
39	12 - R2
40	10 - R2
41	3 - R2
42	6 - R1

Fig. 8b

N	MI1	MI2	MI3
1	0	1	1
2	1	1	0
3	0	0	0
4	1	0	0
5	0	1	1
6	0	0	0
7	0	1	0
8	1	0	1
9	1	0	0
10	1	0	1
11	0	1	0
12	0	0	0
13	0	0	0
14	1	0	0

1 = inversion
0 = inchangé

Fig.8c

RC
0
0
1
0
1
0
1
0
0
1
1
1
1
0

Fig. 9

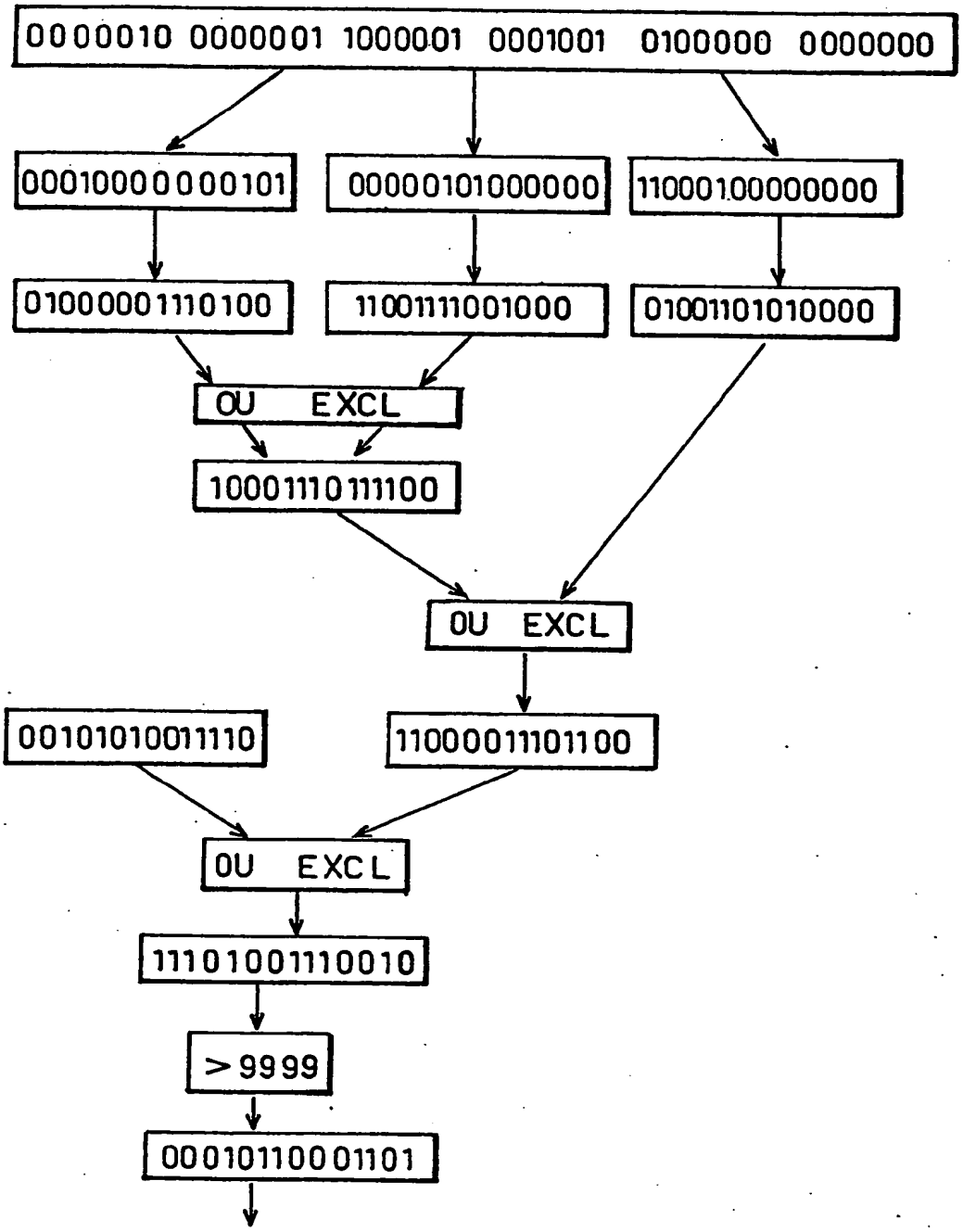


Fig.10